PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-183866
(43)Date of publication of application : 30.06.2000

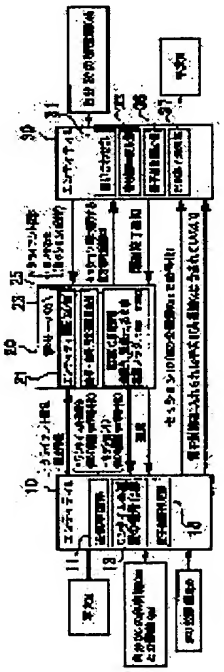
(51)Int.CI. H04L 9/08
G09C 1/00
H04L 9/14

(21)Application number : 10-351857
(22)Date of filing : 10.12.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : HATAJIMA TAKASHI

(54) METHOD AND SYSTEM FOR CIPHER COMMUNICATION, AND RECORDING MEDIUM STORED WITH CIPHER COMMUNICATION PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To confirm if a communication sentence is transferred to the other party being safe and legal by generating either a common key or a session ID and transmitting the communication text with either of them utilized for an electronic envelope.
SOLUTION: A transmission application part 11 of an entity A10 transmits destination information to a key server C20 and requests client authentication. A decoding part 13 of a one-time common key decodes a one-time common key Kc transmitted from the server C20 and takes out the key Kc. And, an electronic envelope preparing part 15 enters a communication text M of plaintext to be transmitted to a receiving client B by a transmitting client A into an electronic envelope E and directly transmits it to an entity B30 without going through the server C20. Further, a key use state managing part 25 issues a session ID which is generated by a random number generator including a session ID proper to this transaction and is enciphered to a public key with the public key Kpc of the server C20 and a public key Kpb of the transmission destination entity B30 in each transmission destination.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－183866
（P2000－183866A）
(43)公開日　平成12年６月30日(2000.6.30)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｃ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｅ	
					６６０Ｇ	
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	9/00	６０１Ｅ	
					６４１	

審査請求　未請求　請求項の数12　ＯＬ　（全８頁）

(21)出願番号　特願平10－351857

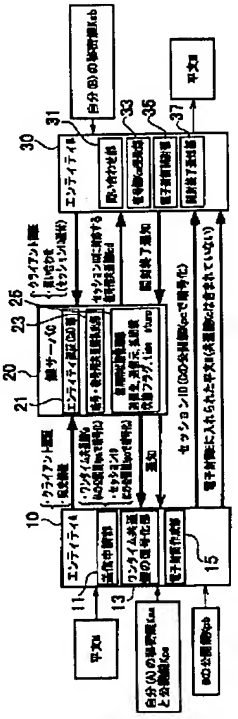
(22)出願日　平成10年12月10日(1998.12.10)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　畑島　隆
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

Ｆターム(参考)　5J104 AA01 AA16 EA02 EA19 EA23 NA02 NA03 NA27 PA07

(54)【発明の名称】　暗号通信方法およびシステムと暗号通信プログラムを記録した記録媒体

(57)【要約】
【課題】　本発明は、より安全でかつ正当な相手に届けられたか送達確認が可能な暗号通信方法およびシステムと暗号通信プログラムを記録した記録媒体を提供することを目的としたものである。
【解決手段】　電子封筒を用いて伝達文を送信元から送信先に送信するときの暗号通信システムであって、少なくとも共通鍵とＩＤのいずれか一つを生成する鍵サーバを送信元と送信先との間に設け、送信元から送信先に送信する際に、鍵サーバで生成された共通鍵または／およびＩＤを電子封筒に利用して伝達文を送信することを特徴とする。



1

【特許請求の範囲】

【請求項１】　伝達文を電子封筒に入れて送信元から送信先に送信するときの暗号通信方法であって、
送信元から送信先に送信する際に、少なくとも共通鍵とセッションＩＤのいずれか一つを生成すると共に、少なくともそのいずれかを電子封筒に利用して伝達文を送信することを特徴とする暗号通信方法。

【請求項２】　前記送信元は、共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成することを特徴とする請求項１記載の暗号通信方法。

【請求項３】　前記共通鍵とセッションＩＤが鍵サーバで生成されるとき、送信先は、送信先から送られてきたセッションＩＤによる鍵サーバへの問い合わせの結果、鍵サーバから送られてきた送信先の公開鍵により公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得るとき、鍵サーバへ開封終了通知を行い、この開封終了通知を受けた鍵サーバは送信元へ着信完了通知を送ることを特徴とする請求項１記載の暗号通信方法。

【請求項４】　伝達文を電子封筒に入れて送信元から送信先に送信するときの暗号通信方法であって、
送信元から送信先に電子封筒を送信する際に、セッションＩＤを都度生成し、このセッションＩＤを同送することにより暗号通信のセッション管理を行うことを特徴とする暗号通信方法。

【請求項５】　前記セッション管理は、鍵サーバの公開鍵で暗号化されたセッションＩＤを暗号通信のトランザクションの際に受け渡すことで行うことを特徴とする請求項４記載の暗号通信方法。

【請求項６】　電子封筒を用いて伝達文を送信元から送信先に送信するときの暗号通信システムであって、
少なくとも共通鍵とセッションＩＤのいずれか一つを生成する鍵サーバを送信元と送信先との間に設け、送信元から送信先に送信する際に、鍵サーバで生成された共通鍵または／およびＩＤを電子封筒に利用して伝達文を送信することを特徴とする暗号通信システム。

【請求項７】　前記共通鍵が鍵サーバで生成されるとき、前記送信元は、共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成することを特徴とする請求項６記載の暗号通信システム。

【請求項８】　前記共通鍵が鍵サーバで生成されるとき、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得ることを特徴とする請求項７記載の暗号通信システム。

【請求項９】　前記共通鍵とセッションＩＤが鍵サーバで生成されるとき、前記送信元は鍵サーバが自身の秘密鍵により公開鍵暗号化した共通鍵払い出しに対するセッションＩＤを送信先へ伝達文とともに送り、送信先は送信元から送付されたセッションＩＤを鍵サーバへ送り、鍵サーバは自身の秘密鍵で復号化して得られる平文のセッションＩＤに対応する共通鍵を送信先の公開鍵で暗号化して送信先へ送り、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封して平文の伝達文を得、さらに送信先は復号完了の後に鍵サーバに前記セッションＩＤを送り返し、鍵サーバは送信元へ着信・復号完了通知を送ることを特徴とする請求項８記載の暗号通信システム。

【請求項１０】　伝達文を電子封筒に入れて送信元から送信先に送信する際に、少なくとも共通鍵とセッションＩＤのいずれか一つを生成すると共に、少なくともそのいずれかを電子封筒に利用して伝達文を送信する暗号通信プログラムを記録した記録媒体。

【請求項１１】　伝達文を電子封筒に入れて送信元から送信先に送信する際に、共通鍵を生成すると共に、送信元はこの共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成して伝達文を送信する暗号通信プログラムを記録した記録媒体。

【請求項１２】　伝達文を電子封筒に入れて送信元から送信先に送信する際に、共通鍵とセッションＩＤが鍵サーバで生成され、この鍵サーバは送信元へ着信完了通知を送り、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得る暗号通信プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、電子封筒を用いた暗号通信の際の安全性を高めると共に、送信先への送達完了を確認し得るようにした暗号通信方法およびシステムと暗号通信プログラムを記録した記録媒体に関するものである。

【０００２】

【従来の技術】従来、電子封筒を用いた暗号通信としては、Ｓ／ＭＩＭＥ（Secure/Multipurpose Internet Mail Extersions）が安全なメッセージ送信方式の一つとして知られている。このＳ／ＭＩＭＥは、公開鍵暗号、共通鍵暗号、一方向暗号を使用して、文書の暗号化と改竄、成りすましを防止している。具体的には、図３および図４に示すように、Ｓ／ＭＩＭＥでは、共通鍵Ｋｃは送信先の公開鍵Ｋｐｂで暗合化され、電子封筒Ｅに内包されて、平文の伝達文Ｍと共に送信先へ送信される。このため、電子封筒Ｅが解読されたら、共通鍵Ｋｃが判るため、確実に解読されてしまうことになる。

【０００３】また、通信路を暗号化するものとしては、ＳＳＬ（Secure Sockets Layer）が知られるが、これ

は、例えばクライアントとサーバとの間で、クライアント認証およびデータについて認証が行われる場合のような、一対一通信にのみ適用が可能である。

【０００４】

【発明が解決しようとする課題】上述したような暗号通信に対して、安全性に不安がある、送達確認ができない、正当な相手に届けられたかが分からない、そのため厳密な商取引には向かない等の問題点が指摘されていた。

【０００５】本発明は、上記課題に鑑みてなされたもので、より安全でかつ正当な相手に届けられたか送達確認が可能な暗号通信方法およびシステムと暗号通信プログラムを記録した記録媒体を提供することを目的としたものである。

【０００６】

【課題を解決するための手段】前述した目的を達成するために、本発明のうちで請求項１記載の発明は、伝達文を電子封筒に入れて送信元から送信先に送信するときの暗号通信方法であって、送信元から送信先に送信する際に、少なくとも共通鍵とセッションＩＤのいずれか一つを生成すると共に、少なくともそのいずれかを電子封筒に利用して伝達文を送信することを要旨とする。

【０００７】請求項１記載の本発明にあっては、少なくとも共通鍵とセッションＩＤのいずれか一つが電子封筒に利用されることから、より安全でおよび／または送達確認が可能となる。

【０００８】請求項２記載の発明は、前記送信元は、共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成することを要旨とする。

【０００９】請求項２記載の本発明にあっては、共通鍵が送信先の公開鍵で暗号化されることからより安全性を高めることができる。

【００１０】請求項３記載の発明は、前記共通鍵とセッションＩＤが鍵サーバで生成されるとき、送信先は、送信先から送られてきたセッションＩＤによる鍵サーバへの問い合わせの結果、鍵サーバから送られてきた送信先の公開鍵により公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得るとき、鍵サーバへ開封終了通知を行い、この開封終了通知を受けた鍵サーバは送信元へ着信完了通知を送ることを要旨とする。

【００１１】請求項３記載の本発明にあっては、セッションＩＤがハンドリングされることから、伝達文の送信先への着信を確実に確認することができる。

【００１２】請求項４記載の発明は、伝達文を電子封筒に入れて送信元から送信先に送信するときの暗号通信方法であって、送信元から送信先に電子封筒を送信する際に、セッションＩＤを都度生成し、このセッションＩＤを同送することにより暗号通信のセッション管理を行うことを要旨とする。

【００１３】請求項５記載の発明は、前記セッション管理は、鍵サーバの公開鍵で暗号化されたセッションＩＤを暗号通信のトランザクションの際に受け渡すことで行うことを要旨とする。

【００１４】請求項６記載の発明は、電子封筒を用いて伝達文を送信元から送信先に送信するときの暗号通信システムであって、少なくとも共通鍵とＩＤのいずれか一つを生成する鍵サーバを送信元と送信先との間に設け、送信元から送信先に送信する際に、鍵サーバで生成された共通鍵または／およびＩＤを電子封筒に利用して伝達文を送信することを要旨とする。

【００１５】請求項７記載の発明は、前記共通鍵が鍵サーバで生成されるとき、前記送信元は、共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成することを要旨とする。

【００１６】請求項８記載の発明は、前記共通鍵が鍵サーバで生成されるとき、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得ることを要旨とする。

【００１７】請求項９記載の発明は、前記共通鍵とセッションＩＤが鍵サーバで生成されるとき、前記送信元は鍵サーバが自身の秘密鍵により公開鍵暗号化した共通鍵払い出しに対するセッションＩＤを送信先へ伝達文とともに送り、送信先は送信元から送付されたセッションＩＤを鍵サーバへ送り、鍵サーバは自身の秘密鍵で復号化して得られる平文のセッションＩＤに対応する共通鍵を送信先の公開鍵で暗号化して送信先へ送り、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封して平文の伝達文を得、さらに送信先は復号完了の後に鍵サーバに前記セッションＩＤを送り返し、鍵サーバは送信元へ着信・復号完了通知を送ることを要旨とする。

【００１８】請求項１０記載の発明は、伝達文を電子封筒に入れて送信元から送信先に送信する際に、少なくとも共通鍵とセッションＩＤのいずれか一つを生成すると共に、少なくともそのいずれかを電子封筒に利用して伝達文を送信する暗号通信プログラムを記録した記録媒体であることを要旨とする。

【００１９】請求項１１記載の発明は、伝達文を電子封筒に入れて送信元から送信先に送信する際に、共通鍵を生成すると共に、送信元はこの共通鍵を送信先の公開鍵で暗号化し、電子封筒を作成して伝達文を送信する暗号通信プログラムを記録した記録媒体であることを要旨とする。

【００２０】請求項１２記載の発明は、伝達文を電子封筒に入れて送信元から送信先に送信する際に、共通鍵と

セッションＩＤが鍵サーバで生成され、この鍵サーバは送信元へ着信完了通知を送り、送信先は鍵サーバから送られた公開鍵暗号化された共通鍵を自身の秘密鍵を用いて復号し、この復号された共通鍵と送信元の公開鍵を用いて電子封筒を開封し、平文の伝達文を得る暗号通信プログラムを記録した記録媒体であることを要旨とする。

【００２１】請求項１０，１１，１２記載の本発明にあっては、暗号通信プログラムを記録媒体として記録しているため、該記録媒体を利用して、その暗号通信プログラムの流通性を高めることができる。

【００２２】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００２３】図１は本発明の一実施の形態に係る暗号通信システムの構成を示すブロック図である。

【００２４】本実施形態の暗号通信システムは、送信クライアントＡの送信端末として機能するエンティティＡ１０、セッション管理機能を持つ鍵サーバＣ２０及び受信クライアントＡの受信端末として機能するエンティティＢ３０によって構成される。また鍵サーバＣ２０はエンティティＡ１０とエンティティＢ３０との間に設けられる。なお、後述するように本実施形態では、セッションＩＤは、鍵サーバＣ２０が鍵サーバ自身の公開鍵Ｋｐで公開鍵暗号化したものであり、送信元、送信先ではともに復号することはないものである。また、同様に共通鍵Ｋｃは、鍵サーバＣ２０が送付相手の公開鍵Ｋｐで公開鍵暗号化したものであり、送り付けられた人は自身の秘密鍵Ｋｓを用いて復号することができる。

【００２５】また、エンティティＡ１０は、送信申請部１１、ワンタイム共通鍵の復号化部１３及び電子封筒作成部１５を有し、鍵サーバＣ２０は、エンティティ認証（ＣＡ）部２１、鍵利用状態管理部２３を有し、さらにエンティティＢ３０は問い合わせ部３１、復号鍵受取部３３、電子封筒開封部３５及び開封終了通知部３７を有している。

【００２６】エンティティＡ１０の送信申請部１１は送信クライアントＡから伝達文の送信の依頼があったときに鍵サーバＣ２０に対し宛先情報を送信すると共にクライアント認証を依頼する機能を有し、ワンタイム共通鍵の復号化部１３は鍵サーバＣ２０から送信されたワンタイム共通鍵Ｋｃ（自身、つまり送信クライアントＡの公開鍵Ｋｐａで暗号化されている）を復号し、ワンタイム共通鍵Ｋｃを取り出す機能を有し、電子封筒作成部１５は送信クライアントＡが受信クライアントＢに送信しようとしている平文の伝達文Ｍ（以下、単に平文Ｍ）を電子封筒Ｅに入れ、鍵サーバＣ２０を介すること無く直接エンティティＢ３０に対し送信する機能を有する。

【００２７】また、鍵サーバＣ２０のエンティティ認証（ＣＡ）部２１は、各エンティティの認証、つまり該鍵サーバＣ２０が予め発行したクライアント証明書について認証する機能を有し、暗号・復号用共通鍵払出部２３は送信側に対しては暗号用の共通鍵Ｋｃを、受信側に対しては復号用の共通鍵Ｋｃを生成し払い出す機能を有し、鍵利用状態管理部２５は本トランザクションに固有なセッションＩＤを内蔵する乱数発生器により発生し、鍵サーバＣ２０の公開鍵Ｋｐｃで公開鍵暗号化したセッションＩＤと、送信先エンティティＢ３０の公開鍵Ｋｐｂとを送信先ごとに発行する機能を有する。

【００２８】さらに、エンティティＢ３０の問い合わせ部３１は先にエンティティＡ１０から送信されたセッションＩＤ（鍵サーバＣ２０の公開鍵Ｋｐｃで暗号化されている）を鍵サーバＣ２０に送付し問い合わせを行う機能を有し、復号鍵受取部３３は鍵サーバＣ２０に送付したセッションＩＤに対応する復号用共通鍵Ｋｃｄ（エンティティＢ３０の公開鍵Ｋｐｂで暗号化されている）を鍵サーバＣ２０から受け取る機能と、暗号化されている復号用の共通鍵Ｋｃｂを自身の秘密鍵で復号する機能を有し、電子封筒開封部３５はエンティティＡ１０から送信された電子封筒Ｅを受信すると共に開封する機能を有し、開封終了通知部３７は電子封筒開封部３５における開封処理を受けて鍵サーバＣ２０に開封終了通知を送信する機能を有する。

【００２９】次に図２を参照して、本実施形態をより具体的に処理手順に従って説明する。本実施形態では各エンティティ（送信元エンティティＡ１０、送信先エンティティＢ３０）は、予め、それぞれ鍵サーバＣ２０（図２では実際に鍵サーバとして機能するエンティティＣを鍵ブローカとして記載している）から電子証明書の発行を受けている。

【００３０】まず、送信元エンティティＡ１０は、ステップＳ１で鍵サーバＣ２０に対し送信先エンティティＢ３０を申告する。

【００３１】鍵サーバＣ２０は、ステップＳ２で送信元エンティティＡ１０の認証を行い、該認証が正常に終了したときには、本トランザクションにのみ有効な共通鍵Ｋｃを、エンティティＡ１０の公開鍵Ｋｐａで暗号化して送信元エンティティＡ１０に送付する。また、このとき本トランザクションに固有なセッションＩＤを乱数発生器により発生し、鍵サーバＣ２０の公開鍵Ｋｐｃで暗号化したセッションＩＤと、送信先エンティティＢ３０の公開鍵Ｋｐｂを送信元エンティティＡ１０に送信する。

【００３２】なお、このとき鍵サーバＣ２０では、送信元エンティティＡ１０からの申告に伴い、送信元（ここではエンティティＡ１０）、送信先（ここではエンティティＢ３０）、要求時刻、発行した共通鍵Ｋｃおよびセッションを鍵利用状態管理部２５に設けられる管理テーブルに記録しておく。また、この管理テーブルへは送信先の数だけレコードを追加するものとする。

【００３３】また、鍵サーバＣ２０から送信元エンティ

ティＡ１０へ送られる共通鍵Ｋｃは、送信元エンティティＡ１０の公開鍵Ｋｐａを用いて公開鍵暗号方式で暗号化されている。また鍵サーバＣ２０からのセッションＩＤも、前述したようにすでに鍵サーバＣ２０の公開鍵Ｋｐｃで公開鍵暗号化されている。

【００３４】次に、ステップＳ３において、送信元エンティティＡ１０は、鍵サーバＣ２０から得たＡの公開鍵Ｋｐａで暗号化した共通鍵Ｋｃを、自身の秘密鍵Ｋｓａを使って復号し、共通鍵Ｋｃとセッションを得る。

【００３５】送信元エンティティＡ１０は、ステップＳ４で、以下に後述するいずれかの手段により選られた（データＡ、Ｂ）、もしくは、（データＣ、Ｄ）の組と共通鍵Ｋｃとをまとめて送信先エンティティＢ３０の公開鍵Ｋｐｂで暗号化し、電子封筒Ｅを作成する。

【００３６】なお、このとき送信元エンティティＡ１０が、以下のいずれかの手段により選られた（データＡ１、Ａ２）、もしくは（データＢ１、Ｂ２）の組をまとめて送信先エンティティＢ３０の公開鍵Ｋｐｂで暗号化し、電子封筒Ｅを作成するようにしても良い。つまり、この実施形態の場合には、共通鍵Ｋｃを電子封筒Ｅに含めていない。

【００３７】（データＡ１、Ａ２）

データＡ１；平文Ｍに対してハッシュ関数を用いて電子署名する。電子署名を送信元エンティティＡ１０の秘密鍵Ｋｓａで公開鍵暗号化する。

データＡ２；平文Ｍを共通鍵Ｋｃで共通鍵暗号化する。

【００３８】（データＢ１、Ｂ２）

データＢ１；平文Ｍを共通鍵Ｋｃで共通鍵暗号化する。

データＢ２；データＢ１をハッシュ関数を用いて電子署名する。電子署名を送信元エンティティＡ１０の秘密鍵Ｋｓａで公開鍵暗号化する。

【００３９】次に、ステップＳ５で、送信元エンティティＡ１０は、セッションＩＤと電子封筒Ｅを送信先エンティティＢ３０へ送信する。

【００４０】送信先エンティティＢ３０は、ステップＳ６で、暗号文が到着したことを鍵サーバＣ２０に通知する。この通知は、前述のセッションＩＤ（鍵サーバＣ２０の公開鍵Ｋｐｃで暗号化したもの）を鍵サーバＣ２０に送信することによって行う。

【００４１】鍵サーバＣ２０は、ステップＳ７で、受信したセッションＩＤを、自身の秘密鍵Ｋｓで復号化し、平文となったセッションＩＤが記載されているレコードを管理テーブルから探す。このレコードに記載されている共通鍵Ｋｃを送信先エンティティＢ３０の公開鍵Ｋｐｂで公開鍵暗号化して送信先エンティティＢ３０へ送付する。

【００４２】送信先エンティティＢ３０は、ステップＳ８で鍵サーバＣ２０から送られた公開鍵暗号化された共通鍵Ｋｃを、自身の秘密鍵Ｋｓｂを用いて復号する。さらに復号された共通鍵Ｋｃと送信元エンティティＡ１０の公開鍵Ｋｐａを用いて、電子封筒Ｅを開封し、平文Ｍを得る（ステップＳ９）。これにより送信先エンティティＢ３０は、ステップＳ１０で、鍵サーバＣ２０に対して復号完了を通知する（セッションＩＤを送信）。

【００４３】一方、鍵サーバＣ２０は、この復号完了通知を受けて、ステップＳ１１でレコードにある送信元エンティティＡ１０へ着信完了通知を送る。これにより送信元エンティティＡ１０は、伝達文の送信先エンティティＢ３０への送達完了を確認する。なお、このときの通知手段はメール、専用プロトコルなど任意である。この着信完了通知の送信と同時に、鍵サーバＣ２０は管理テーブルからレコードを削除する。

【００４４】次に、他の実施形態について説明する。

【００４５】ステップＳ１乃至７，１０までは、前述した実施形態と同様なので説明を省略する。

【００４６】鍵サーバＣ２０の管理テーブルでは共通鍵送信済みフラグを立て、新規セッションＩＤを公開鍵暗号化して送信先エンティティＢ３０へ送る。

【００４７】送信先エンティティＢ３０は、鍵サーバＣ２０から送られた公開鍵暗号化された共通鍵Ｋｃを、自身の秘密鍵Ｋｓｂを用いて復号する。復号された共通鍵Ｋｃと送信元エンティティＡ１０の公開鍵Ｋｐａを用いて、電子封筒Ｅを開封し、平文Ｍを得る。

【００４８】さらに送信先エンティティＢ３０は復号完了したら、鍵サーバＣ２０に通信新規セッションＩＤを送り返す。これにより鍵サーバＣ２０は送信元エンティティＡ１０へ着信・復号完了通知を送る。このときの通信手段はメール、専用プロトコルなど任意である。

【００４９】なお、上述したきたような暗号通信システムは暗号通信プログラムにより実現され、該プログラムは記録媒体に記録して提供される。

【００５０】上述してきたように、上記各実施形態によれば、鍵サーバからのＩＤ払い出しにより、セッション管理を可能にし、また鍵サーバにしか解読できないセッションＩＤをハンドリングすることによって通信セッション全体について安全性を確保している。すなわち、セッション管理により、いわゆる配達証明を可能にしたものである。

【００５１】また、電子封筒に共通鍵を内包しない場合、電子封筒だけが解読されても、共通鍵を手に入れないと、内容を平文に出来ない分だけＳ／ＭＩＭＥよりも解読が難しくなる。つまり、本文を高速な共通鍵暗号で暗号化するＳ／ＭＩＭＥの利点を生かしつつ安全性を高めたことになる。

【００５２】さらに共通鍵は信頼できる鍵サーバから別途送られるため、攻撃される確率を低く出来、また共通鍵はトランザクション中の鍵受取者の公開鍵で暗号化されるため鍵受取者以外は復号することはできない。

【００５３】耐成りすまし性は、電子証明書と、サーバにしか解読できないセッションＩＤによる認証により確

保され、また耐改竄性は一方向暗号と電子証明書により安全性を保証している。

【００５４】これを通常の郵便（郵政省管轄）になぞらえると、Ｓ／ＭＩＭＥが（書留郵便＋内容証明）であるのに対し、本発明は（書留郵便＋内容証明＋配達証明）と表現される。

【００５５】

【発明の効果】以上説明したように、本発明によれば、安全かつメッセージが送達されたことが確認可能な暗号通信システムを構築できる。

【図面の簡単な説明】

【図１】本発明に係る暗号データメッセージングシステムの一実施形態の全体構成図である。

【図２】本発明に係る暗号データメッセージングシステムの一実施形態における処理を示したデータフロー図である。

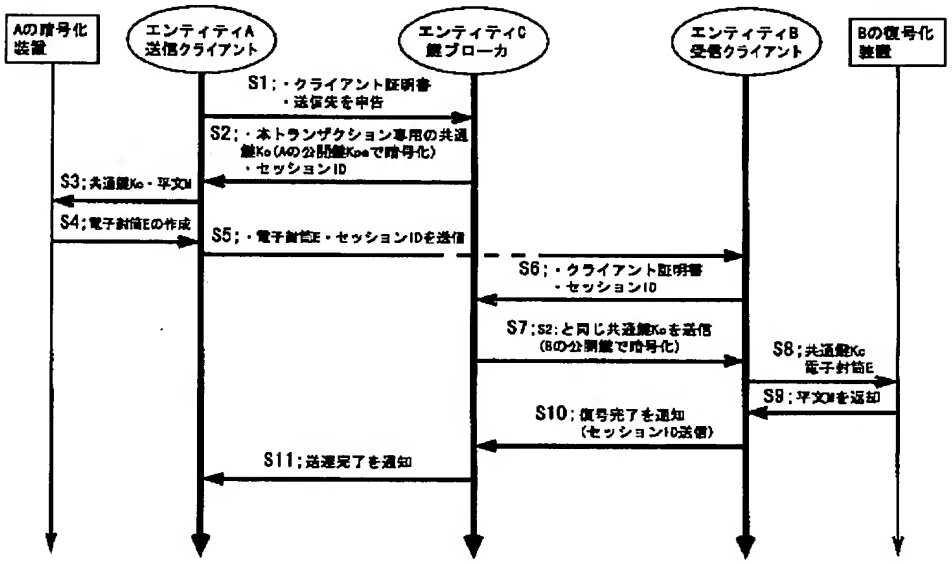
【図３】従来の暗号データメッセージングシステムの全体構成を示すブロック図である。

【図４】従来の暗号データメッセージングシステムにおける処理を示したデータフロー図である。

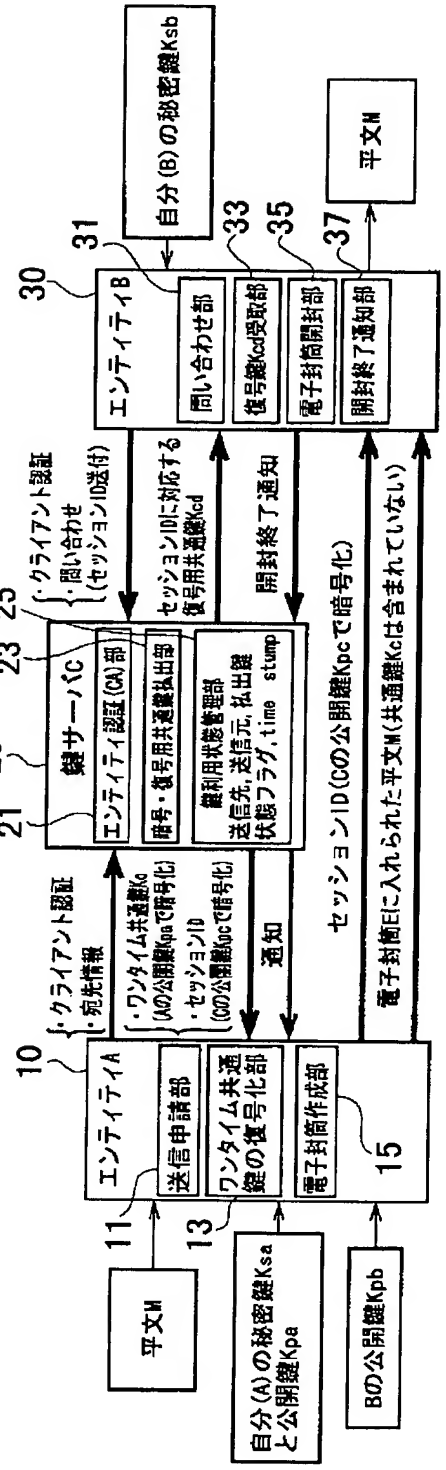
【符号の説明】

１０　エンティティＡ
１１　送信申請部
１３　ワンタイム共通鍵の復号化部
１５　電子封筒作成部
２０　鍵サーバＣ
２１　エンティティ認証（ＣＡ）部
２３　鍵利用状態管理部
３０　エンティティＢ
３１　問い合わせ部
３３　復号鍵受取部
３５　電子封筒開封部
３７　開封終了通知部

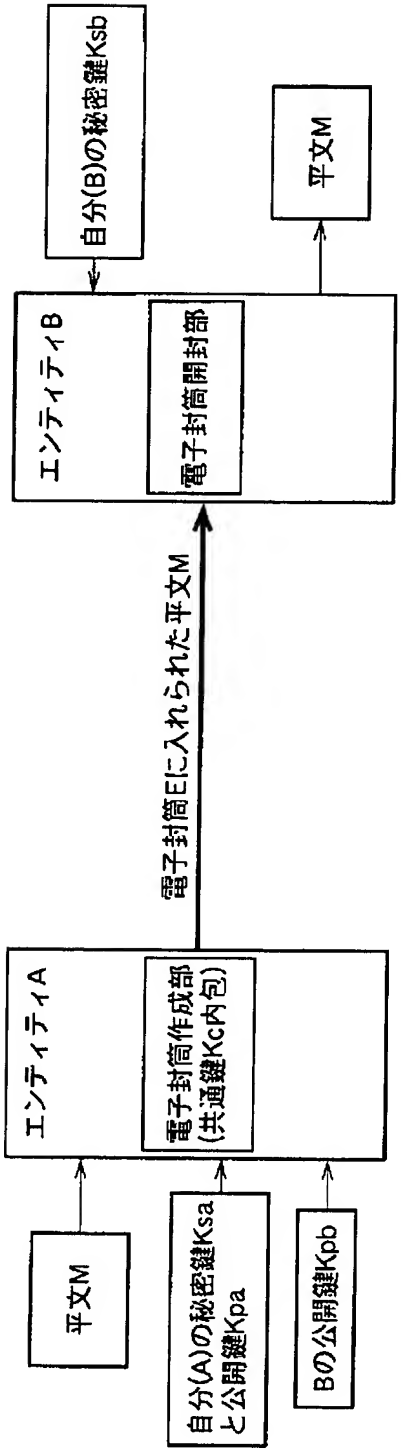
【図２】



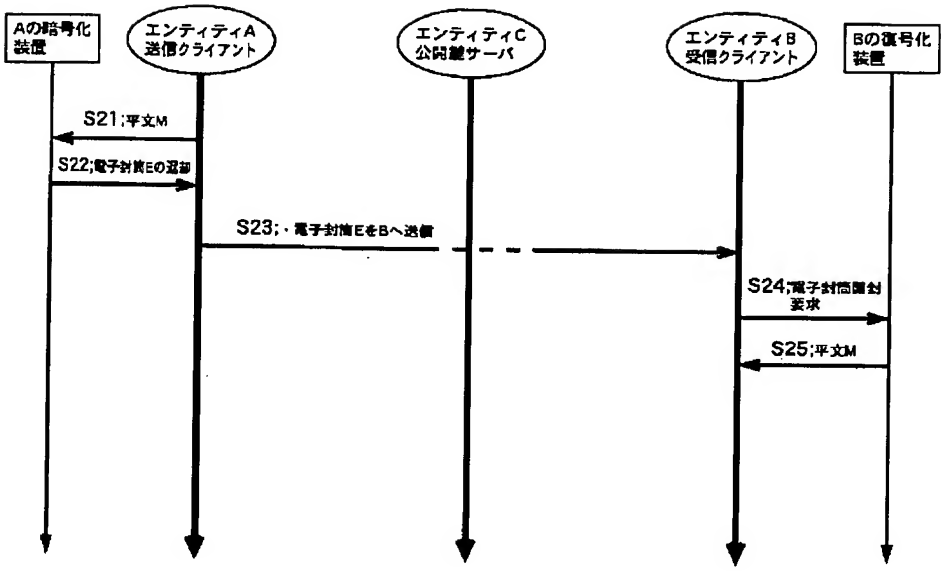
【図１】


エンティティA
10
送信申請部
11
ワンタイム共通鍵の復号化部
13
電子封筒作成部
15
・クライアント認証
・宛先情報
・ワンタイム共通鍵c (AのB公開鍵Kpaで暗号化)
・セッションID (CのB公開鍵Kpcで暗号化)
通知
セッションID(CのB公開鍵Kpcで暗号化)
電子封筒Eに入れられた平文M(共通鍵Kcは含まれていない)
鍵サーバC
20
エンティティ認証(CA)部
21
暗号・復号用共通鍵払出部
23
鍵利用状態管理部
送信先,送信元,払出鍵
状態フラグ,time stump
25
・クライアント認証
・問い合わせ
(セッションID送付)
セッションIDに対応する復号用共通鍵Kcd
開封終了通知
エンティティB
30
問い合わせ部
31
復号鍵Kcd受取部
33
電子封筒開封部
35
開封終了通知部
37
平文M
自分(B)の秘密鍵Ksb
平文M
自分(A)の秘密鍵Ksaと公開鍵Kpa
B公開鍵Kpb

【図３】


自分(B)の秘密鍵Ksb
エンティティB
電子封筒開封部
平文M
電子封筒Eに入れられた平文M
エンティティA
電子封筒作成部(共通鍵Kc内包)
平文M
自分(A)の秘密鍵Ksaと公開鍵Kpa
B公開鍵Kpb

【図４】


Aの暗号化装置
エンティティA送信クライアント
エンティティC公開鍵サーバ
エンティティB受信クライアント
Bの復号化装置
S21;平文M
S22;電子封筒Eの送信
S23;・電子封筒EをBへ送信
S24;電子封筒開封要求
S25;平文M